Breaking a novel colour image encryption algorithm based on chaos

Chengqing Li[a,b,*], Yu Zhang[c], Rong Ou[a], Kwok-Wo Wong[d]

[a] *College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China*
[b] *MOE (Ministry of Education) Key Laboratory of Intelligent Computing and Information Processing, Xiangtan University, China*
[c] *School of Mathematics and Computational Science, Xiangtan University, Xiangtan 411105, Hunan, China*
[d] *Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China*

Abstract

Recently, a colour image encryption algorithm based on chaos was proposed by cascading two position permutation operations and one substitution operation, which are all determined by some pseudo-random number sequences generated by iterating the Logistic map. This paper evaluates the security level of the encryption algorithm and finds that the position permutation-only part and the substitution part can be separately broken with only $\lceil(\log_2(3MN))/8\rceil$ and 2 chosen plain-images, respectively, where MN is the size of the plain-image. Concise theoretical analyses are provided to support the chosen-plaintext attack, which are verified by experimental results also.

Keywords: image encryption, chaos, cryptanalysis, chosen-plaintext attack

1. Introduction

Security of multimedia data (image, video, audio/speech) become more and more important as it is transmitted over all kinds of wired/wireless networks more and more frequently. Both design and security analysis of multimedia encryption algorithms have been received keen attention of the related researchers in the past decade [1, 2, 3, 4, 5]. Due to the subtle similarity between some dynamical properties of chaos, like sensitivity to changes of initial condition and control parameter of chaotic systems, and the basic properties of cryptography, diffusion and confusion, chaos was considered as a special way to design secure and efficient encryption algorithm [6, 7, 8]. As image data is a representative form of multimedia data, and it helps to show the claimed good performances of the proposed encryption algorithms, most chaos-based encryption algorithms adopt image data as encryption object.

According to the record of *Web of Science*, more than four hundred papers on designing chaos-based image encryption schemes were published between 1997 and 2011 (inclusive). Meanwhile, no more than one hundred and half papers on security analysis of chaos-based image encryption schemes were published. Short of scrutiny on the security makes many chaos-based image encryption schemes are insecure against some conventional attacks, such as known/chosen-plaintext attack and chosen-ciphertext attack [9, 10, 11, 12]. Some representative chaos-based encryption algorithms and a general framework evaluating security of this class of encryption algorithms were concluded in [13]. In many chaos-based image encryption algorithms, a chaos system, composed of one or more chaotic maps, is used to generate pseudo-random number sequence (PRNS), which is then adopted to determine and control combination of some basic encryption functions [14, 15]. In digital domain, finite precision computation and quantization process make some dynamical properties of chaos system be degenerated in some form, which may cause potential threat to security of the chaos-based encryption algorithms [16].

The present paper analyzes the security of the image encryption algorithms proposed in [17] and finds that the three basic encryption operations of the algorithm are all *key-invertible*, i.e. the unknown information controlling an encryption operation can be derived directly from the input and its output result. Furthermore, the three encryption functions are run independently. So, the position permutation part and the substitution part of the image encryption algorithm under study can be broken separately with a few chosen plain-images. Both detailed theoretical analyses and experimental results are presented to support the chosen-plaintext attack.

The rest of this paper is organized as follows. The next section introduces the image encryption algorithm un-

[*] Corresponding author.
Email address: chengqingg@gmail.com (Chengqing Li)

der study briefly. Section 3 presents an efficient chosen-plaintext attack on the encryption algorithm with some experimental results. The last section concludes the paper.

2. The colour image encryption algorithm under study

The plaintext of the encryption algorithm under study is a RGB colour image of size $M \times N$ (height×width), which can be represented as a $M \times N \times 3$ matrix of pixel values $\boldsymbol{I} = \{I(i,j,k)\}_{i=0,j=0,k=0}^{M-1,N-1,2} = \{(R(i,j), G(i,j), B(i,j))\}_{i=0,j=0}^{M-1,N-1}$. Similarly, the corresponding cipher-image is denoted by $\boldsymbol{I}' = \{I'(i,j,k)\}_{i=0,j=0,k=0}^{M-1,N-1,2} = \{(R'(i,j), G'(i,j), B'(i,j))\}_{i=0,j=0}^{M-1,N-1}$. Then, the colour image encryption algorithm under study can be described as follows[1].

- *The secret key* is composed of two positive integers m_1, m_2, and two sets of initial condition and control parameter of the logistic map

$$f(x) = \mu \cdot x \cdot (1-x), \tag{1}$$

  (x_0, μ_0), (x_0^*, μ_0^*), where $x_0, x_0^* \in (0,1)$, and $\mu_0, \mu_0^* \in (3.5699456, 4)$.

- *The initialization procedure*:

  (1) Iterate the logistical map (1) m_1 times from initial condition x_0 to obtain a new initial condition under fixed control parameter μ_0. Then, further iterate it $3M$ times to get a chaotic states sequence $\{X_l\}_{l=0}^{3M-1}$. Finally, a permutation sequence $\{T_l\}_{l=0}^{3M-1}$ is derived by comparing $\{X_l\}_{l=0}^{3M-1}$ and its sorted version, where X_{T_l} is the l-th largest element in the sequence $\{X_l\}_{l=0}^{3M-1}$.

  (2) Iterate the logistical map (1) m_2 times from initial condition x_0^* to obtain a new initial condition under fixed control parameter μ_0^*. Then, further iterate it $3MN$ times to get a chaotic states sequence $\{X_l^*\}_{l=0}^{3MN-1}$. For $i = 0 \sim M-1$, obtain another permutation sequence $\{T_{i,l}^*\}_{l=0}^{3N-1}$ by comparing $\{X_{3iN+l}^*\}_{l=0}^{3N-1}$ and its sorted version, where $X^*_{3iN+T^*_{i,l}}$ is the l-th largest elements in sequence $\{X^*_{3iN+l}\}_{l=0}^{3N-1}$.

  (3) Generate a PRNS $\{Y_l\}_{l=0}^{3MN-1}$ from the sequence $\{X_l^*\}_{l=0}^{3MN-1}$ via $Y_l = \lfloor X_l^* \cdot 10^{14} \rfloor \bmod 3$, where

$$(a \bmod b) = a - b \cdot \lfloor a/b \rfloor$$

  when $b \neq 0$.

  (4) To make the numbers of the three different elements in $\{Y_l\}_{l=0}^{3MN-1}$ are all equal to MN, update the last $3MN-1$ elements as follows: for $l = 1 \sim 3MN-1$, set

$$Y_l = \begin{cases} 1, & \text{if } Y_l = 0, n_0 \geq MN \text{ and } n_1 < MN, \\ 2, & \text{if } Y_l = 0, n_0 \geq MN \text{ and } n_1 \geq MN, \\ 2, & \text{if } Y_l = 1, n_1 \geq MN \text{ and } n_2 < MN, \\ 0, & \text{if } Y_l = 1, n_1 \geq MN \text{ and } n_2 \geq MN, \\ 0, & \text{if } Y_l = 2, n_2 \geq MN \text{ and } n_0 < MN, \\ 1, & \text{if } Y_l = 2, n_2 \geq MN \text{ and } n_0 \geq MN, \end{cases}$$

  where n_0, n_1, n_2 represent the number of 0, 1, 2 in $\{Y_i\}_{i=0}^{l-1}$, respectively.

  (5) Generate another PRNS $\{Z_l\}_{l=0}^{3MN-1}$ from the sequence $\{X_l^*\}_{l=0}^{3MN-1}$ via $Z_l = \lfloor X_l^* \cdot 10^{14} \rfloor \bmod 256$.

- *The encryption procedure* is a simple concatenation of the following three encryption operations.

  (1) *Row permutation:* for $i = 0 \sim M-1$, $j = 0 \sim N-1$, $k = 0 \sim 2$, set

$$I^*(i,j,k) = I(i^*, j, k^*),$$

  where $i^* = T_{kM+i} \bmod M, k^* = \lfloor T_{kM+i}/M \rfloor$.

  (2) *Column permutation:* for $i = 0 \sim M-1$, $j = 0 \sim N-1$, $k = 0 \sim 2$, set

$$I^{**}(i,j,k) = I^*(i, j^{**}, k^{**}),$$

  where $j^{**} = T^*_{i,kN+j} \bmod N, k^{**} = \lfloor T^*_{i,kN+j}/N \rfloor$.

  (3) *Substitution:* First, let

$$I'(0,0,Y_0) = (I^{**}(0,0,Y_0) + Z_0) \bmod 256. \tag{2}$$

  Then, one pixel is selected iteratively from the other un-encrypted pixels of the intermediate image $\boldsymbol{I}^{**} = \{I^{**}(i,j,k)\}_{i=0,j=0,k=0}^{M-1,N-1,2}$ according to a PRNS $\{Y_l\}_{l=1}^{3MN-1}$, determining which channel's pixel is chosen. The selected pixels are encrypted by the previous selected pixel, the corresponding cipher-pixel and a pseudo-random number as follows: calculate

$$\begin{aligned} I'(i,j,k) = (I^{**}(i,j,k) + I^{**}(i',j',k') \\ + I'(i',j',k') + Z_l) \bmod 256 \end{aligned} \tag{3}$$

  for $l = 1 \sim 3MN-1$, where

$$\begin{aligned} i &= \lfloor n_k/N \rfloor, & j &= n_k \bmod N, & k &= Y_l, \\ i' &= \lfloor n_{k'}/N \rfloor, & j' &= n_{k'} \bmod N, & k' &= Y_{l-1}, \end{aligned}$$

  n_k and $n_{k'}$ represent the number of k and k' in $\{Y_t\}_{t=0}^{l}$ and $\{Y_t\}_{t=0}^{l-1}$, respectively.

[1] To make the presentation more concise and complete, some notations in the original paper [17] are modified under the condition that essential form of the encryption algorithm is kept unchanged.

- *The decryption procedure* is similar to the encryption one except the following points: (1) the above encryption operations are run in a reverse order; (2) the permutation sequences are replaced by their invertible versions; (3) equation (2) and Eq. (3) are replaced by

$$I^{**}(0,0,Y_0) = (I'(0,0,Y_0) - Z_0) \bmod 256$$

  and

$$\begin{aligned} I^{**}(i,j,k) = (I'(i,j,k) - I^{**}(i',j',k') \\ - I'(i',j',k') - Z_l) \bmod 256, \end{aligned}$$

  respectively.

3. Chosen-plaintext attack

In [17, Sec. 3.2.6], it is claimed that the image encryption algorithm under study is robust against chosen-plaintext attack based on the following two points: (a) the used PRNSs are all sensitive to changes of secret key; (b) the substitution function (3) owns a feed-back mechanism. However, we will show that the claim is not right in this section. As the image encryption algorithm under study is composed of three independent encryption operations, the position permutation part and the substitution part can be broken separately with a strategy of *Divide and Conquer*.

As for plain-images of fixed value, both the *Row permutation* and the *Column permutation* are canceled and only the *Substitution* is left. Assume two chosen plain-images of fixed value $\boldsymbol{I}_1 = \{I_1(i,j,k) \equiv d_1\}$, $\boldsymbol{I}_2 = \{I_2(i,j,k) \equiv d_2\}$ are available. From Eq. (2), one has

$$I_1'(0,0,Y_0) = (I_1(0,0,Y_0) + Z_0) \bmod 256 \tag{4}$$

and

$$I_2'(0,0,Y_0) = (I_2(0,0,Y_0) + Z_0) \bmod 256. \tag{5}$$

Subtract Eq. (5) from Eq. (4), one has

$$(I_1'(0,0,Y_0) - I_2'(0,0,Y_0)) \in \{D, D-256, D+256\}, \tag{6}$$

where $D = d_1 - d_2$. Referring to Eq. (3), one has

$$\begin{aligned} I_1'(i,j,k) = (I_1(i,j,k) + I_1(i',j',k') \\ + I_1'(i',j',k') + Z_l) \bmod 256, \end{aligned} \tag{7}$$

$$\begin{aligned} I_2'(i,j,k) = (I_2(i,j,k) + I_2(i',j',k') \\ + I_2'(i',j',k') + Z_l) \bmod 256 \end{aligned} \tag{8}$$

for $l = 1 \sim 3MN-1$, where (i,j,k) and (i',j',k') are determined by $\{Y_t\}_{t=0}^{l}$ and $\{Y_t\}_{t=0}^{l-1}$ respectively, as the above section. Subtract Eq. (8) from Eq. (7), one has

$$(I_1'-I_2')(i,j,k) \equiv (2D + (I_1'-I_2')(i',j',k')) \pmod{256} \tag{9}$$

where $(I_1' - I_2')(i,j,k) = I_1'(i,j,k) - I_2'(i,j,k)$, and $(I_1' - I_2')(i',j',k') = I_1'(i',j',k') - I_2'(i',j',k')$, the same hereinafter.

Then, a property of $(I_1' - I_2')$ can be presented as follows.

Property 1. *Difference between the cipher-images of* $\boldsymbol{I}_1$ *and* $\boldsymbol{I}_2$ *satisfies that*

$$(I_1' - I_2')(i,j,Y_l) \equiv ((2l+1)D) \pmod{256} \tag{10}$$

for $l = 0 \sim 3MN-1$, *where* $(i,j) = (0,0)$ *when* $l = 0$, $(i,j) = (\lfloor (n_{Y_l}+1)/N \rfloor, (n_{Y_l}+1) \bmod N)$ *otherwise, and* n_{Y_l} *denotes the number of the elements in* $\{Y_t\}_{t=0}^{l-1}$, *whose values are equal to* Y_l.

Proof. This property can be proved via mathematical induction on l. When $l = 0$, one can get

$$(I_1' - I_2')(0,0,Y_0) \equiv D \pmod{256}$$

from Eq. (6), which means Eq. (10) holds for $l = 0$. Assume Eq. (10) holds for $l = l^*$, i.e.,

$$(I_1' - I_2')(i,j,Y_{l^*}) \equiv ((2l^*+1)D) \pmod{256}$$

where $l^* < 3MN-1$. Then, let us study the case for $l = (l^*+1)$. From Eq. (9), one has

$$\begin{aligned} (I_1' - I_2')(i,j,Y_{l^*+1}) &\equiv (2D + (I_1' - I_2')(i,j,Y_{l^*})) \pmod{256} \\ &= ((2(l^*+1)+1)D) \pmod{256}. \end{aligned}$$

This completes the mathematical induction, hence finishes the proof of the property. □

Utilizing Property 1, one can get the estimated version of Y_0,

$$\widehat{Y_0} = \begin{cases} 0 & \text{if } (I_1' - I_2')(0,0,0) \equiv D \pmod{256}, \\ 1 & \text{if } (I_1' - I_2')(0,0,1) \equiv D \pmod{256}, \\ 2 & \text{if } (I_1' - I_2')(0,0,2) \equiv D \pmod{256}, \end{cases} \tag{11}$$

when $D \neq 128$. Obviously, one can assure $\widehat{Y_0} = Y_0$ definitely when

$$\#(\{k \mid (I_1' - I_2')(0,0,k) \equiv D \pmod{256}\}) = 1, \tag{12}$$

where $\#(\cdot)$ denotes the cardinality of a set. Once the value of Y_0 is determined, the estimated values of $\{Y_l\}_{l=1}^{3MN-1}$, $\{\widehat{Y_l}\}_{l=1}^{3MN-1}$, can be obtained in order with the similar method, namely set

$$\widehat{Y_l} = k \quad \text{if } (I_1' - I_2')(i_k, j_k, k) \equiv ((2l+1)D) \pmod{256}$$

for $l = 1 \sim 3MN-1$, where $i_k = \lfloor (n_k+1)/N \rfloor$, $j_k = (n_k+1) \bmod N$, and n_k represents the number of k in $\{\widehat{Y_t}\}_{t=0}^{l-1}$.

Referring to [18, Sec. 5.4], one can get period of the sequence $\{(2l^*+1)D) \bmod 256\}_{l^*=0}^{3MN-1}$, $T = \frac{256}{2 \cdot \gcd(D,256)} = \frac{128}{\gcd(D,256)}$. To help estimate success probability of this attack, we give another property of $(I_1' - I_2')$ as follows.

Property 2. *Inequality*

$$\#\left(\{k \mid (I'_1 - I'_2)(i_k, j_k, k) \equiv ((2l^* + 1)D) \pmod{256}\}\right) > 1$$

holds if and only if

$$Y_{l^*+S} \notin \{Y_l\}_{l=l^*}^{l^*+S-1}, \tag{13}$$

where $(S \bmod T) = 0$, $i_k = \lfloor (n_k + 1)/N \rfloor$, $j_k = (n_k + 1) \bmod N$*, and* n_k *represents the number of* k *in* $\{Y_t\}_{t=0}^{l^*-1}$.

Proof. Assume, for the purpose of contradiction, that certain l^* satisfies $Y_{l^*+S} \notin \{Y_l\}_{l=l^*}^{l^*+S-1}$ and such that

$$\#\left(\{k \mid (I'_1 - I'_2)(i_k, j_k, k) \equiv ((2l^* + 1)D) \pmod{256}\}\right) = 1.$$

From Property 1 and the hypothesis, one has

$$(2l^* + 1)D \neq (2(l^* + S) + 1)D \pmod{256},$$

which leads to

$$0 \neq 2SD \pmod{256}.$$

Then, one has

$$\begin{aligned}(S \bmod T) &= S \bmod \frac{128}{\gcd(D, 256)}\\ &= (2SD) \bmod \frac{2D \cdot 128}{\gcd(D, 256)}\\ &= (2SD) \bmod \left(256 \cdot \frac{D}{\gcd(D, 256)}\right)\\ &\neq 0,\end{aligned}$$

thereby contradicting with the given condition. So, the property is proved. □

Assume that Y_l uniformly distributes over $\{0, 1, 2\}$ for $l = 0 \sim 3MN - 1$, one can calculate the probability that condition (13) in Property 2 hold for a given l^* and T,

$$Prob\left[Y_{l^*+S} \notin \{Y_l\}_{l=l^*}^{l^*+S-1}\right] = \left(\left(\frac{2}{3}\right)^{kT} \cdot \frac{1}{3}\right),$$

where $k \in \{1, \cdots, \lfloor 2MN/T \rfloor\}$. Then, an upper bound of the probability that condition (13) hold can be got as

$$Prob(MN) = \sum\nolimits_{k=1}^{\lfloor 2MN/T \rfloor} (3MN - kT)\left(\left(\frac{2}{3}\right)^{kT} \cdot \frac{1}{3}\right).$$

When $T = 128$, one can calculate $Prob(2272 \cdot 1704) \approx 1.1173 \cdot 10^{-16}$ for a relatively big plain-image of size 2272 × 1704. As for plain-images of smaller size, one can assure that the success probability of this attack is much bigger than $(1 - 1.12 \cdot 10^{-16})$ due to that the following points hold at the same time.

- The upper bound probability $Prob(MN)$ is a strictly increasing function with respect to MN;
- Even Eq. (13) holds, $\widehat{Y}_l^* = Y_l^*$ would still happen with probability $\frac{1}{2}$ or $\frac{1}{3}$;
- The value of $Prob(MN)$ is calculated by summarizing the probability of some cases that may happen simultaneously.

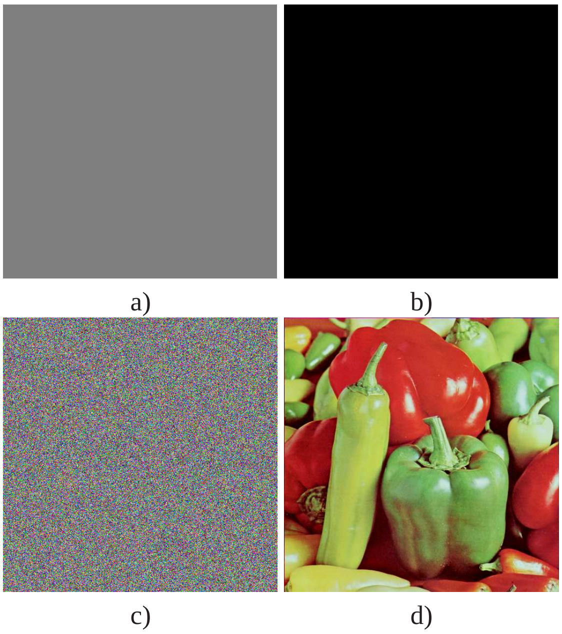
Based on the above analysis, one can conclude that breaking of the *Substitution* part can be implemented successfully with an extremely high probability.

Once the equivalent secret key determining *Substitution* is recovered, the image encryption algorithm under study becomes a position permutation-only gray-scale image encryption algorithm composing of the *Row permutation* and the *Column permutation*. Considering the number of possible positions of every plain-pixel is $3MN$, the bit length of each element of chosen plaintext should be $\lceil \log_2(3MN) \rceil$ to assure that every permuted elements are different from each other. As bit size of every channel of plain-image is fixed to 8, only $\lceil (\log_2(3MN))/8 \rceil$ pairs of chosen plain-images are required to recover the equivalent version of $\{T_l\}_{l=0}^{3M-1}$ and $\{T^*_{i,l}\}_{i=0,l=0}^{M-1,3N-1}$. Referring to quantitative cryptanalysis of permutation-only encryption algorithms in [19, 20], the complexity of breaking the position permutation part is only $O(3MN)$.

To validate the performance of the proposed attack, a great number of experiments on some plain-images of size 512 × 512 were made with some randomly selected secret keys. When $\mu_0 = 4.0$, $x_0 = 0.123456789764$, $m_1 = 1000$, $\mu_0^* = 3.999999$, $x_0^* = 0.567891234567$ and $m_2 = 2000$, two chosen plain-images of fixed pixel value 127 and 0, shown in Fig. 1a) and b) respectively, are used to recover the PRNS $\{Y_l\}_{l=0}^{3MN-1}$. Then, $\lceil (\log_2(3 \times 2^9 \cdot 2^9))/8 \rceil = 3$ pairs of chosen plain-image are constructed to recover the equivalent secret of the position permutation-only part. Finally, the equivalent versions of the sub-keys controlling two main encryption parts are used together to break a cipher-image encrypted with the same secret key, which is shown in Fig. 1c). The decryption result is shown in Fig. 1d) and it is identical with the original plain-image, which verifies the effectiveness of the proposed attack.

4. Conclusion

This paper studied the security of a novel colour image encryption algorithm based on chaos proposed in [17]. It is found that the encryption algorithm can be broken with chosen-plaintext attack efficiently. The number of required chosen plain-images and complexity of the attacking are



a) b) c) d)

Figure 1: Chosen-plaintext attack: a) the chosen plain-image of fixed value 127; b) the chosen plain-image of fixed value 0; c) the cipher-image of plain-image "Baboon"; d) the recovered plain-image of the image shown in Fig. 1c).

proportional to a logarithm of size of plain-images and the size, respectively. As a conclusion, the image encryption algorithm under study is not suggested in serious applications requiring a high level of security.

Acknowledgement

This research was supported by the National Natural Science Foundation of China (No. 61100216), Scientific Research Fund of Hunan Provincial Education Department (No. 11B124), and Start-up Fund of Xiangtan University (Nos. 10QDZ39, 10QDZ40).

References

[1] Y. Mao, M. Wu, A joint signal processing and cryptographic approach to multimedia encryption, IEEE Transactions on Image Processing 15 (7) (2006) 2061–2075.

[2] G. Jakimoski, K. Subbalakshmi, Cryptanalysis of some multimedia encryption schemes, IEEE Transactions on Multimedia 10 (3) (2008) 330–338.

[3] J. Zhou, O. C. Au, P. H.-W. Wong, Adaptive chosen-ciphertext attack on secure arithmetic coding, IEEE Transactions on Signal Processing 57 (5) (2009) 1825–1838.

[4] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Processing 90 (9) (2010) 2714–2722.

[5] T. Stutz, A. Uhl, A survey of H.264 AVC/SVC encryption, IEEE Transactions on Circuits and Systems for Video Technology, doi:10.1109/TCSVT.2011.2162290 (2011).

[6] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons & Fractals 21 (3) (2004) 749–761.

[7] X. Tong, M. Cui, Image encryption scheme based on 3d baker with dynamical compound chaotic sequence cipher generator, Signal Processing 89 (4) (2009) 480–491.

[8] J. Chen, J. Zhou, K.-W. Wong, A modified chaos-based joint compression and encryption scheme, IEEE Transactions on Circuits and Systems II 58 (2) (2011) 110–114.

[9] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos 18 (3) (2008) art. no. 033112.

[10] C. Li, S. Li, G. Chen, W. A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image and Vision Computing 27 (8) (2009) 1035–1039.

[11] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image and Vision Computing 27 (9) (2009) 1371–1381.

[12] E. Solak, C. Cokal, O. T. Yildiz, T. Biyikoglu, Cryptanalysis of Fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos 20 (5) (2010) 1405–1413.

[13] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (8) (2006) 2129–2151.

[14] C. Li, S. Li, D. Zhang, G. Chen, Cryptanalysis of a data security protection scheme for VoIP, IEE Proceedings-Vis. Image Signal Process 153 (1) (2006) 1–10.

[15] S. M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Processing 92 (5) (2012) 1202–1215.

[16] F. Chen, K.-W. Wong, X. Liao, T. Xiang, Period distribution of generalized discrete arnold cat map for N=pe, IEEE Transactions on Information Theory 58 (1) (2012) 445–452.

[17] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Processing 92 (4) (2012) 1101–1108.

[18] G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, 6th Edition, Oxford University Press, UK, 2008.

[19] S. Li, C. Li, G. Chen, N. G. Bourbakis, K.-T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing: Image Communication 23 (3) (2008) 212–223.

[20] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing 91 (4) (2011) 949–954.